Web Images Maps News Shopping Gmail more ▾ Sign in

Google "side channel" OR ((power OR current) analysis) attack dummy (operation (Search

Web Scholar

Results 1 - 100 of about 32,000 for "side channel" OR ((power OR current) analysis) attack dummy (operat

Scholarly articles for "side channel" OR ((power OR current) analysis) attack dummy (operation OR calculation OR process) parallel :pdf

- A Refined Power-Analysis Attack on Elliptic Curve ... - Goubin - Cited by 83
- The Width-w NAF Method Provides Small Memory and Fast ... - Okeya - Cited by 42
- The Montgomery Powering Ladder - Joye - Cited by 63

[PDF] On the Power of Simple Branch Prediction Analysis
File Format: PDF/Adobe Acrobat - View as HTML
ileged process to attack other processes running in parallel on the same processor ......
analysis: side-channel atomicity. IEEE Transactions on Computers, ...
eprint.iacr.org/2006/351.pdf - Similar pages
by O Aciicmez - Cited by 14 - Related articles - All 5 versions

[PDF] Yet Another MicroArchitectural Attack: Exploiting I-cache
File Format: PDF/Adobe Acrobat - View as HTML
Cache analysis techniques enable an unprivileged process to attack another process,
e.g., a. cipher process, running in parallel on the same processor as ...
eprint.iacr.org/2007/164.pdf - Similar pages
by O Aciicmez - Cited by 3 - Related articles
More results from eprint.iacr.org »

Information Sciences : Efficient elliptic curve scalar ...
To resist a power analysis attack, four countermeasures are presented in the paper. ...
Since our countermeasures need no dummy addition, they can be more ...
linkinghub.elsevier.com/retrieve/pii/S0020025507000084 - Similar pages
by N Zhang - 2007 - Cited by 1 - Related articles - All 2 versions

Design Challenges for a Differential-Power-Analysis Aware GALS ...
Side channel analysis attacks on cryptographic systems, first .... Dummy Operation. Data
I/O. Dummy. Dummy Sub1. Sub3. Dummy. Dummy. Sub4. Dummy. Dummy ...
linkinghub.elsevier.com/retrieve/pii/S1571066106000272 - Similar pages
by FK Gürkaynak - 2006 - Related articles - All 2 versions
More results from linkinghub.elsevier.com »

Improving DPA Security by Using Globally-Asynchronous Locally ...
Side channel analysis attacks, and particularly Differ-. ential Power Analysis (DPA), ... A
DPA attack targets a specific operation of the crypto- ...
ieeexplore.ieee.org/iel5/10265/32889/01541646.pdf?arnumber=1541646 - Similar pages
by F Gurkaynak - 2005 - Cited by 2 - Related articles - All 3 versions

An Overview of Power Analysis Attacks Against Field Programmable ...
The first successful power analysis attack against an FPGA .... surement process in side-
channel attacks. As will be empha-. sized later in the paper, ...
ieeexplore.ieee.org/iel5/5/33381/01580507.pdf - Similar pages
More results from ieeexplore.ieee.org »

Low Voltage Design against Power Analysis Attacks
measures such as random process interrupts, dummy. instructions and random noise
addition have .... a power analysis attack; finally, the paper concludes ...
doi.ieeecomputersociety.org/10.1109/DELTA.2008.50 - Similar pages

by O Mirmotahari - All 2 versions

Micro-Architectural Cryptanalysis
Recent studies on side-channel analysis have led to a new area, ... can run such a spy process to execute dummy instructions in parallel with a cipher ...
doi.ieeecomputersociety.org/10.1109/MSP.2007.91 - Similar pages
by O Aciiçmez - 2007 - Cited by 2 - Related articles - All 4 versions
More results from doi.ieeecomputersociety.org »

[PDF] On the Power of Simple Branch Prediction Analysis
File Format: PDF/Adobe Acrobat - View as HTML
single quasi-parallel computation process, a Simple Branch. Prediction Analysis (SBPA) attack. In order to clearly dif-. ferentiate those branch prediction ...
islab.oregonstate.edu/koc/papers/c40.pdf - Similar pages
by O Aciiçmez - Cited by 14 - Related articles - All 5 versions

[PDF] Predicting Secret Keys Via Branch Prediction
File Format: PDF/Adobe Acrobat - View as HTML
an unprivileged process to attack other processes running in parallel on the ...... venting simple side-channel analysis: side-channel atomicity. ...
islab.oregonstate.edu/koc/papers/c39.pdf - Similar pages
by O Aciicmez - 2007 - Cited by 16 - Related articles
More results from islab.oregonstate.edu »

[PDF] Protecting AES Software Implementations on 32-bit Processors ...
File Format: PDF/Adobe Acrobat - View as HTML
tacks in parallel. The attack can be done by combining the power consumption for the .....
A Side-Channel Analysis Resistant. Description of the AES S-box. ...
www.iaik.tugraz.at/Research/publications/2007/ACNS2007_PAS.pdf - Similar pages
by S Tillich - Cited by 1 - Related articles - All 3 versions

[PDF] Folie 1
File Format: PDF/Adobe Acrobat - View as HTML
Methods to attack cryptographic devices (e.g. power analysis). • Countermeasures .....
Process N additional dummy States. • -> (N+1)*16 possible occurrences ...
www.iaik.tugraz.at/RESEARCH/publications/2007/ACNS2007_PAS_Slides.pdf - Similar pages

[PDF] Proposal for a Ultra Low Voltage NAND gate to withstand Power ...
File Format: PDF/Adobe Acrobat - View as HTML
some information during a power analysis attack. The main. weakness would be in the parallel pullup chain. Simulation. results verifying the ULV NAND gate ...
www.waset.org/ijecs/v1/v1-4-39.pdf - Similar pages
by O Mirmotahari - Related articles - All 2 versions

[PDF] Cache Based Power Analysis Attacks on AES
File Format: PDF/Adobe Acrobat - View as HTML
nisms influence the current to briefly describe the side-channel model. .... With these observations we can build a power analysis attack based on the ...
www.geocities.com/mike.tunstall/papers/FT06.pdf - Similar pages
by J Fournier - Cited by 3 - Related articles

GALS System Design: Side Channel Attack Secure Cryptographic ...
Cryptographic datapaths that process many parallel operations at the same ... between a cryptographic operation from a Dummy Operation (DOP) that does not ...
si2.epfl.ch/~gurkayna/acacia/c3.html - 116k - Cached - Similar pages

GALS System Design: Side Channel Attack Secure Cryptographic ...
3.5.1 Side Channel Attacks 3.5.2 Differential Power Analysis ...... Dummy Operation: Both datapath units process random data, no cryptographic data is ...

si2.epfl.ch/~gurkayna/acacia/acacia.html - 394k - Cached - Similar pages

[PDF] Design Method for Constant Power Consumption of Differential Logic ...
File Format: PDF/Adobe Acrobat - View as HTML
danger that side-channel attacks pose to all embedded. devices [3],[4]. At first, the differential power analysis attack has been ...
www.cosic.esat.kuleuven.be/publications/article-676.pdf - Similar pages
by K Tiri - Cited by 8 - Related articles - All 9 versions

[PDF] Power and Fault Analysis Resistance in Hardware through Dynamic ...
File Format: PDF/Adobe Acrobat - View as HTML
Modified architecture for improved side channel analysis attack resistance ..... process and no remarkable patterns in the power traces in either case. ...
www.cosic.esat.kuleuven.be/publications/article-1128.pdf - Similar pages
More results from www.cosic.esat.kuleuven.be »

On the Power of Simple Branch Prediction Analysis
Nov 22, 2006 ... Very recently, a new software side-channel attack, called Branch ... states through spying on a single quasi-parallel computation process, ...
cryptome.org/sbpa/sbpa.htm - 56k - Cached - Similar pages

[PDF] Differential Power Analysis on Countermeasures Using Binary Signed ...
File Format: PDF/Adobe Acrobat - View as HTML
we extend the proposed attack to the refined power analysis .... The difference between countermeasures using a dummy. operation and the indistinguishable ...
etrij.etri.re.kr/Cyber/servlet/GetFile?fileid=SPF-1191829378087 - Similar pages
by I Introduction - 2007 - Related articles - All 3 versions

Protection against side channel attacks - Patent EP1840732
Well-known side channel attacks include Simple Power Analysis (SPA), ... Thanks to the masking operation, the DPA attack is no longer applicable, ...
www.freepatentsonline.com/EP1840732.html - Similar pages
by G Fumaroli - 2007 - All 3 versions

Information processor and instruction fetch control method ...
The side channel attack is an attack that tries to obtain internal secret ...... calculation result is dealt with as the dummy operation (the operation ...
www.freepatentsonline.com/y2008/0140995.html - Similar pages
by H Fukazawa - 2008
More results from www.freepatentsonline.com »

[PDF] Aspects of Public Key Cryptosystems in Practice
File Format: PDF/Adobe Acrobat - View as HTML
Side Channel Attacks - SPA and Timing Attack. n. SPA: Simple Power Attack. K. Attack: ... Introduce dummy operation to "homogenize" the point operations ...
www.cacr.math.uwaterloo.ca/conferences/2000/ecc2000/hess.pdf - Similar pages

[PDF] Design Principles for Tamper-Resistant Smartcard Processors ...
File Format: PDF/Adobe Acrobat - View as HTML
Parallel encryption or background dummy operations introduce non-determinism ... Non-invasive attacks (glitching, current analysis) are the main concern ...
www.cl.cam.ac.uk/~mgk25/sc99-tamper-slides.pdf - Similar pages
by O Kömmerling - Cited by 74 - Related articles - All 7 versions

[PDF] Balanced Self-Checking Asynchronous Logic for Smart Card Applications
File Format: PDF/Adobe Acrobat - View as HTML
Power analysis attacks are prevented by removing or hiding information leaked by such ..... consumption during writes may be balanced using dummy circuitry, ...
www.cl.cam.ac.uk/~rja14/Papers/micromicro2003.pdf - Similar pages
by S Moore - Cited by 40 - Related articles - All 15 versions

More results from www.cl.cam.ac.uk »

[PDF] The Smart Card Platform
File Format: PDF/Adobe Acrobat - View as HTML
Routine. Programming. dummy cell. Process. completed. yes. Process ... SPA (Simple Power Analysis). Obtaining information about the secret key by direct ...
www.etsi.org/WebSite/document/Workshop/
Security2006/Security2006S1_3_Klaus_Vedder.pdf - Similar pages

[PDF] The Smart Card Platform
File Format: PDF/Adobe Acrobat - View as HTML
attack against just one card, not against the system itself .... SPA (Simple Power Analysis). Obtaining information about the secret key by direct ...
www.etsi.org/WebSite/document/Workshop/
Security2007/Security2007S5_4_Klaus_Vedder.pdf - Similar pages

[PDF] A Collision-Attack on AES Combining Side Channel- and Differential ...
File Format: PDF/Adobe Acrobat - View as HTML
can be detected by power analysis techniques, therefore collision ...... Furthermore, it is possible to apply the optimized attack in parallel against all ...
www.crypto.rub.de/imperia/md/content/texte/publications/conferences/aes_collisions.pdf - Similar pages
by K Schramm - Cited by 23 - Related articles - All 5 versions

[PDF] Improved Elliptic Curve Multiplication Methods Resistant against ...
File Format: PDF/Adobe Acrobat - View as HTML
J. Coron, "Resistance against differential power analysis for elliptic curve ... K. Okeya, and K. Sakurai, "On Insecurity of the Side Channel Attack Coun- ...
www.bmoeller.de/pdf/impr-sca-indocrypt2002.pdf - Similar pages
by T Izu - Cited by 31 - Related articles - All 7 versions

Semiconductor device having power consumption analysis preventing ...
This permits processing time and power consumption for the same process in .... to the target circuit in parallel, the same number of the dummy bit string ...
www.freshpatents.com/Semiconductor-device-having-power-consumption-analysis-preventing-function-dt2008061... - 31k - Cached - Similar pages

[PDF] Microsoft PowerPoint - Aciicmez.ppt
File Format: PDF/Adobe Acrobat - View as HTML
Recently, the Side-Channel attack arena hit the PC as a new. victim platform: ... process is executed in parallel with the crypto process which ...
conferenze.dei.polimi.it/FDTC07/Aciicmez.pdf - Similar pages
by O Aciiçmez - Cited by 4 - Related articles - All 3 versions

[PDF] Memories: a survey of their secure uses in smart cards
File Format: PDF/Adobe Acrobat - View as HTML
adapted the notion of side-channel analysis to smart cards [9], ... power supply and leakage current. This attack can allow. locking out tamper-responding ...
www.dice.ucl.ac.be/crypto/files/publications/pdf166.pdf - Similar pages
by M Neve - Cited by 12 - Related articles - All 6 versions

(WO/2005/029704) A DYNAMIC AND DIFFERENTIAL CMOS LOGIC WITH SIGNAL ...
On the algorithmic level, random process interrupts interleave dummy ..... Electromagnetic Analysis (EMA) is the equivalent of a power attack but instead ...
www.wipo.int/pctdb/en/wo.jsp?IA=WO2005029704&DISPLAY=DESC - 68k - Cached - Similar pages

[PDF] The Predecessor Attack: An Analysis of a Threat to Anonymous ...
File Format: PDF/Adobe Acrobat - View as HTML
In constructing the attack and analysis, we make several simplifying assumptions. about

protocol operation. Specifically, our major assumptions are: ...
www.freehaven.net/anonbib/cache/Wright:2004.pdf - Similar pages
by MK WRIGHT - Cited by 34 - Related articles - All 12 versions

Data processing apparatus and method for operating a data ...
If the CPU does not perform any dummy operation at the time when it is not ... current profile, and for a data processing apparatus with reduced power ...
www.patentstorm.us/patents/7181632-description.html - Similar pages

Predicting secret keys via branch prediction - CiteSeerX
This paper presents a new software side-channel attack — enabled by the ... an unprivileged process to attack other processes running in parallel on the ...
citeseer.ist.psu.edu/758468.html - 27k - Cached - Similar pages

[PDF] GALS System Design: Side Channel Attack Secure Cryptographic ...
File Format: PDF/Adobe Acrobat
thesis only power analysis attacks will be considered as side channel attacks. ...... Dummy Operation: Both datapath units process random data, no cryp- ...
e-collection.ethbib.ethz.ch/ecol-pool/diss/fulltext/eth16351.pdf - Similar pages

[PDF] Side channel attacks
File Format: PDF/Adobe Acrobat
This report describes the current state-of-the-art about side channel crypt- ...... Recently, a new variant of power analysis attack, named template attack, ...
www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf - Similar pages

[PDF] The Montgomery Powering Ladder
File Format: PDF/Adobe Acrobat - View as HTML
regarding some side-channel analysis (e.g., simple power analysis (SPA)) then .... is equal to 0, then this multiplication is a dummy operation ...
www.gemplus.us/smart/rd/publications/pdf/JY03mont.pdf - Similar pages
by M Joye - Cited by 64 - Related articles - All 16 versions

Security tackles smartcard hackers - 06/03/2006 - Electronics Weekly
Mar 6, 2006 ... The best known side-channel attack is differential power analysis (DPA), first described by Paul Kocher in 1998 (this was what Tiri and ...
www.electronicsweekly.com/Articles/2006/03/06/37793/security-tackles-smartcard-hackers.htm - 42k - Cached - Similar pages

[PDF] Timing analysis in low-latency mix networks: attacks and defenses
File Format: PDF/Adobe Acrobat - View as HTML
We will refer to this as the timing analysis attack. .... a dummy packet. Each mix is assumed to have a store of properly encrypted ...
www.cs.utexas.edu/~shmat/shmat_esorics06.pdf - Similar pages
by V Shmatikov - Cited by 9 - Related articles - All 4 versions

[PDF] Secure AES Hardware Module for Resource Constrained Devices
File Format: PDF/Adobe Acrobat - View as HTML
The round key is computed in parallel to the round operation. ...... Messerges, T. S.: Using second-order power analysis to attack DPA resistant soft- ...
www.cs.uku.fi/tutkimus/security/publications/files/lncs3313.pdf - Similar pages
by E Trichina - Cited by 8 - Related articles - All 4 versions

[PDF] Macro-Micro Correlation Analysis for Detecting Network Security ...
File Format: PDF/Adobe Acrobat - View as HTML
analysis. Flow of. micro. analysis. Dummy email. accounts ... Dispatched process for. new attack pattern. Over 10000 parallel CPD processes ...
www.laas.fr/IFIPWG/Workshops&Meetings/50/workshop/08%20Nakao.pdf - Similar pages

[PDF] Elliptic Curves and SideChannel Analysis
File Format: PDF/Adobe Acrobat - View as HTML
The basic operation in elliptic curve cryptography is the scalar ... power analysisi.e. a simple sidechannel analysis using power consumption as ...
www.gemplus.com/smart/rd/publications/pdf/Joy03ecc.pdf - Similar pages
by M Joye - Cited by 8 - Related articles - All 10 versions

[PDF] Cache Attacks and Countermeasures: the Case of AES (Extended ...
File Format: PDF/Adobe Acrobat - View as HTML
Keywords: side-channel attack, cache, memory access, cryptanalysis, AES ...... accesses, e.g., by performing a dummy encryption in parallel to the real one. ...
people.csail.mit.edu/tromer/papers/cache.pdf - Similar pages
by DA Osvik - Cited by 71 - Related articles - All 18 versions

[PDF] Power Analysis in Cryptography
File Format: PDF/Adobe Acrobat - View as HTML
all 128 bits of the key if attacked at the calculation of PE(x, y), ... Thomas Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant ...
ece.gmu.edu/courses/ECE543/project/reports_2000/lash_report.pdf - Similar pages

[PDF] arXiv:cs/0102012v1 [cs.CR] 16 Feb 2001
File Format: PDF/Adobe Acrobat - View as HTML
A slightly different attack known as. the differential power analysis monitors the power ...... parallel to the axis of possible states of the system. ...
arxiv.org/pdf/cs.CR/0102012 - Similar pages
by NS Philip - 2001 - Cited by 4 - Related articles - All 3 versions

[PDF] Secure Health Data Linkage and Geocoding: Current Approaches and ...
File Format: PDF/Adobe Acrobat - View as HTML
might also add chaff to their data in the form of dummy records to obfuscate ... the third party, Carol, could mount a frequency analysis attack against the ...
datamining.anu.edu.au/publications/2006/ehPass2006.pdf - Similar pages
by P Christen - Cited by 1 - Related articles - All 4 versions

[PDF] CMP Aware RC Extraction
File Format: PDF/Adobe Acrobat - View as HTML
guard band through more accurate timing/power analysis. CMP model based approach. also helps dummy fill optimization as compared to current rule (density) ...
www.venusmultimedia.net/cadence/cmp.pdf - Similar pages

IEICE Technical Committee Submission System - VLSI Design ...
Countermeasures against Side Channel Attack are necessary to achieve .... of the FIR filter designed using the conventional parallel operation units, w. ...
www.ieice.org/ken/program/index.php?instsoc=IEICE-A&tgid=IEICE-VLD&year=5&region=0&sch1=1... - 285k - Cached - Similar pages

[PDF] &
File Format: PDF/Adobe Acrobat - View as HTML
conductor device with stress, Simple Power Analysis. (SPA) and Differential Power Analysis .... circuit in parallel and its corresponding dummy serial in- ...
https://publications.european-patent-office.org/PublicationServer/getpdf.jsp?cc=EP&pn=1760595&ki=A1 - Similar pages

[PDF] Key Randomization Countermeasures to Power Analysis Attacks on ...
File Format: PDF/Adobe Acrobat
Side-Channel Analysis. SPA. Simple Power Analysis ...... current point operation is an addition or a doubling. The attack applies if the key ...
uwspace.uwaterloo.ca/bitstream/10012/2772/1/thesis.pdf - Similar pages
by NM Ebeid - Cited by 1 - Related articles - All 4 versions

[PDF] ORNL/TM-2004/042 Metals and Ceramics Division Correlation of ...
File Format: PDF/Adobe Acrobat - View as HTML
was also evaluated via correlation coefficient analysis for all pairs of process variables with. several delay times considered. The value of current noise ...
www.osti.gov/energycitations/servlets/purl/885546-ML6go4/885546.PDF - Similar pages
by SJ Pawel - 2004 - All 2 versions

Measuring Morbidity: Disease Counts, Binary Variables, and ...
The other major approach has been to use dummy variables for each illness to ..... For the count variables, the power calculation is based on the following ...
psychsoc.gerontologyjournals.org/cgi/content/full/55/3/S173 - Similar pages
by KF Ferraro - 2000 - Cited by 31 - Related articles - All 2 versions

[PDF] Analyzing Performance Vulnerability due to Resource Denial-of ...
File Format: PDF/Adobe Acrobat - View as HTML
the performance of the application running on the victim core. 4.6 Attack Using Locked Atomic Operation. To implement the atomic operation, ...
www.eecg.toronto.edu/~moshovos/CMPMSI07/DongHyukWoo-DoS.pdf - Similar pages
by DH Woo - Cited by 5 - Related articles

AERADE
Various dummy stings were tested on the rear of a related series of ... Also presented is an analysis of jet duplication by use of a sting. View PDF ...
aerade.cranfield.ac.uk/results.php?Simplequery=afterbody - 18k - Cached - Similar pages

Strategic Effects for Dummies: A novice's approach to effects ...
Also, because an OODA is a continuous process, it is possible to attack the same OODA at more than one node at a time. These are two ways a parallel attack ...
www.airpower.maxwell.af.mil/airchronicles/cc/Hill.html - 73k - Cached - Similar pages
by MT Tighe - Related articles

[PDF] SPA - A Synthesisable Amulet Core for Smartcard Applications
File Format: PDF/Adobe Acrobat - View as HTML
leakage through variations in power supply current or elec-. tromagnetic radiation [17]. This form of attack relies on. two features of the circuit under ...
ftp://ftp.cs.man.ac.uk/pub/amulet/papers/SPA.pdf - Similar pages
by LA Plana - Cited by 29 - Related articles - All 3 versions

[PDF] P5Cx012/02x/40/73/80/144 family Secure dual interface and contact ...
File Format: PDF/Adobe Acrobat
calculation speed for RSA and ECC as well as availability of secure hardware support for ..... Differential Fault Analysis. DPA. Differential Power Analysis ...
www.nxp.com/acrobat_download/datasheets/
P5CX012_02X_40_73_80_144_FAM_SDS_3.pdf - Similar pages

[PDF] “Killer App” of Wearable Computing: Wireless Force Sensing Body ...
File Format: PDF/Adobe Acrobat - View as HTML
This allows multiple signals to be process in parallel .... Our current recommendation. is 8 watts as the power threshold for a scored hit for ...
www-users.cs.umn.edu/~echi/papers/2004-UIST/2004-UIST-SensorHogu.pdf -
Similar pages
by EH Chi - Cited by 12 - Related articles - All 11 versions

The 40-mg dose of eletriptan: comparative efficacy and ...
parallel-group, double-dummy design in which the. double-blind was maintained by matching ..... current analysis provide reassurance that this is not the ...
www.blackwell-synergy.com/doi/pdf/10.1046/j.1351-5101.2003.00730.x - Similar pages
by HC Diener - 2004 - Cited by 17 - Related articles - All 8 versions

[PDF] The self-synchronizing stream cipher Mosquito: eSTREAM ...
File Format: PDF/Adobe Acrobat - View as HTML
Finally we discuss some modes of operation to use Mosquito for ...... be vulnerable especially with respect to differential power analysis and differential ...
www.ecrypt.eu.org/stream/p3ciphers/mosquito/mosquito.pdf - Similar pages
by J Daemen - Related articles - All 4 versions

[PDF] Physical Design of Cryptographic Applications: Constrained ...
File Format: PDF/Adobe Acrobat
Power analysis attacks is a class of side-channel attacks that exploits infor- ...... and a reduced swing current mode operation allowing dynamic power ...
edoc.bib.ucl.ac.be:81/ETD-db/collection/available/BelnUcetd-04212008-114433/unrestricted/thesis.pdf - Similar pages
by M Francois

"Index". In: Smart Card Handbook (Third Edition)
differential fault analysis, 550. differential power analysis, 537 ..... Operation and maintenance center, 741. Optical fault induction attack, 552 ...
doi.wiley.com/10.1002/047085670X.index - Similar pages
by AE Standard

[PDF] Using Attack Injection to Discover New Vulnerabilities
File Format: PDF/Adobe Acrobat - View as HTML
collection and analysis of the responses. In more detail,. Test level The test manager controls the whole process of. attack injection. ...
www.di.fc.ul.pt/~nuno/PAPERS/DSN06_aject.pdf - Similar pages
by N Neves - Cited by 10 - Related articles - All 9 versions

[PDF] How To Avoid Seven Deadly Sins in the Study of Behavior
File Format: PDF/Adobe Acrobat - View as HTML
tested singly after a dummy predator attack. Imagine that we do not find .... statistical power analysis and include the necessary information in the ...
evolution.unibe.ch/teaching/ExpDesign/Milinski_ASB1997_teach.pdf - Similar pages
by M MILINSKI - Cited by 17 - Related articles

Science Links Japan | Joho Shori Gakkai Shinpojiumu Ronbunshu
Responsive Multithreaded Processor for Parallel/Distributed Real-Time Processing .... Power Analysis on Randomized Base Selection Method of Residue Number ...
sciencelinks.jp/j-east/journal/J/Y0978B/2004.php - 104k - Cached - Similar pages
by BT Opening - Cited by 2 - Related articles

Secure data processing unit, and an associated method Number ...
The best known current profile analysis methods are, in this case, ... such attacks on data processing units in security-relevant fields of operation, ...
www.linkgrinder.com/Patents/Secure_data_pro_7412608.html - 79k - 23 hours ago - Cached - Similar pages

[PDF] Elliptic Curves and Side-Channel Attacks
File Format: PDF/Adobe Acrobat - View as HTML
The basic operation in elliptic curve cryptography is the scalar multiplication, ... power analysis (i.e., a simple side-channel analysis using power ...
math2007.univ-rennes1.fr/crypto/2003-04/rennes.pdf - Similar pages
by M Joye - Cited by 1 - Related articles

[PDF] Data Remanence in Semiconductor Devices
File Format: PDF/Adobe Acrobat - View as HTML
amount of power supply current being supplied to the device, known as I .... approach is to have the crypto processor process dummy data ...
www.cypherpunks.to/~peter/usenix01.pdf - Similar pages

by P Gutmann - Cited by 41 - Related articles - All 12 versions

[PDF] Autonomous on-wafer sensors for process modeling, diagnosis, and ...
File Format: PDF/Adobe Acrobat - View as HTML
during design and development of process equipment. The. current equipment development procedure involves processing. a set of dummy wafers, measuring the ...
bcam.berkeley.edu/ARCHIVE/journal/autonomous%20on.pdf - Similar pages
by M Freed - 2001 - Cited by 16 - Related articles - All 11 versions

[PDF] A Dynamic and Differential CMOS Logic Style to Resist Power and ...
File Format: PDF/Adobe Acrobat - View as HTML
On the algorithmic level, random process interrupts interleave dummy instruc- ..... [7] T.S. Messerges, “Using Second-Order Power Analysis to Attack DPA ...
mirror.cr.yp.to/eprint.iacr.org/2004/066.pdf - Similar pages
by K Tiri - Cited by 1 - Related articles - All 3 versions

A practical implementation of the timing attack — CiteSeerX ...
In this paper, power analysis techniques used to attack DES are reviewed and ... an unprivileged process to attack other processes running in parallel on ...
citeseerx.ist.psu.edu/showciting;jsessionid=1E61313CBE807A175F5A022842F32835?cid=142253 - 42k - Cached - Similar pages

Statistical Data Analysis
Developments in the field of statistical data analysis often parallel or follow .... A socalled Generalized Gaussian distribution has the following pdf ...
home.ubalt.edu/ntsbarsh/stat-data/Topics.htm - 307k - Cached - Similar pages

Hack MCU: Cipher Instruction Search Attack on the Bus-Encryption ...
For the attack, we connect most pins of the DS5002FP CPU and two pins of each SRAM chip to a special read-out device. The CPU power supply has to be ...
www.mikahk.com/topics/hack-mcu.asp - 46k - Cached - Similar pages

[PDF] Security in Distributed Embedded Systems
File Format: PDF/Adobe Acrobat - View as HTML
security in software as well as side-channel attacks have been devised thus, ... service attack, but also power analysis, packet transmission, ...
dspace.hh.se/dspace/bitstream/2082/1758/1/Security%20in%20Distributed%20Embedded%20Systems.pdf - Similar pages
by R Tewatia - 2008

FM 90-2 Chapter 5 Deception Means
Two items commonly used in visual deception are dummies and decoys. ..... Th operation plan called for 10th Army to make a two-corps attack on the west side ...
fas.org/irp/doddir/army/fm90-2/90-2ch5.htm - 43k - Cached - Similar pages

[PDF] Static Timing Analysis Based Transformations of Super-Complex ...
File Format: PDF/Adobe Acrobat - View as HTML
The execution delays. used for energy calculation were previously discussed and shown in Table 1. Table 4: Functional Unit Power Estimates. Operation. Power ...
etd.library.pitt.edu/ETD/available/etd-03102008-120235/unrestricted/ColinIhrig-ms-3-18-08.pdf - Similar pages
by CJ Ihrig - 2008

[PDF] Multilevel modelling in the analysis of observational datasets in ...
File Format: PDF/Adobe Acrobat
Approach to conventional analysis regression analyses 30. Approach to multilevel modelling 33. Predictive power of multilevel vs conventional models 39 ...
pages.unibas.ch/diss/2007/DissB_7939.pdf - Similar pages
by MM Schwenkglenks - Related articles

[PDF] 1 Grid- and Dummy-Cluster-Based Learning of Normal and Intrusive ...
File Format: PDF/Adobe Acrobat - View as HTML
A simple method of incrementally clustering data points is to process data ..... numbers of data points in dummy cluster j and c respectively, if current ...
www-personal.engin.umd.umich.edu/~xylum/
WorkingPapers/Li&Ye_QREI_CCAS_Grid&Dummy.pdf - Similar pages

Demagoguery for (academically-inclined) dummies | Re:harmonized
The overdetermined analysis that makes an open-and-shut case for the prosecution ... Make full use of labels, both for their reductive power and to make ...
reharmonized.an-earful.com/demagoguery-for-dummies/ - Similar pages

CRYPTO '99
For ISO-9796-2 and a modified version of Ecash, this attack is better than all ...... Differential Power Analysis, Paul Kocher, Joshua Jaffe, Benjamin Jun ...
www.ieee-security.org/Cipher/ConfReports/1999/CR1999-crypto99.html - 70k - Cached - Similar pages

[PDF] The Role of Instincts
File Format: PDF/Adobe Acrobat
collocated themselves parallel to the dummy maintaining the characteristic ... We can thus, refer to stimulus for escaping, motivation to attack and so on. ...
www.tdx.cesca.es/TESIS_UB/AVAILABLE/TDX-0420105-161934//03.ROLE_OF_INSTINCTS.pdf - Similar pages

[PDF] A Generalized Model for Polymorphic Ciphers
File Format: PDF/Adobe Acrobat
Differential Power Analysis (DPA): DPA is a new kind of attack on Smart Card .... The compiling process of the keystream generator can be generalized as ...
www.pmc-ciphers.com/vpics/9a8f098c615a425eab6d17c804dd67ae/
whitepapers/roellgen02generalizedPMCmodel.pdf - Similar pages
by CB Roellgen - Cited by 1 - Related articles - All 11 versions

Design Automation of Real-Life Asynchronous Devices and Systems
(3) Robustness to process and operation variations that are ...... tion combines high differential power analysis (DPA) attack resistance ...
www.nowpublishers.com/getpdf.aspx?doi=1000000006&product=EDA - Similar pages
by A Taubin - Related articles - All 7 versions

Date Title Authors Theme ID 2005-09-22 A Formal Approach to Fault ...
... power 528 2004-04-15 Gate Oxide Leakage Current Analysis and Reduction for ..... 272 2002-09-02 Hierarchical Dummy Fill for Process Uniformity Y. Chen, ...
www.gigascale.org/pubs/745/all_by_date.txt - 124k - Cached - Similar pages
by DS Blaauw

Is Gender Subordinate to Class? an Empirical Assessment of Colvin ...
(51) This latter group is dropped from the current analysis, as are youths ... The dummy code measure of youth bonds to parental authority (PARENINF) is ...
www.questia.com/PM.qst?a=o&se=gglsc&d=5000299807 - Similar pages
by SS Simpson - 1994 - Cited by 9 - Related articles - All 4 versions

[PDF] Open Smart Card Infrastructure for Europe
File Format: PDF/Adobe Acrobat - View as HTML
Side-Channel analysis [12] is a form of attack against secure tokens by which .... Power Consumption. Typically, current products based on contactless ...
dematerialisedid.com/PDFs/OSCIE/Download/06-2.PDF - Similar pages

Korean War - Wikipedia, the free encyclopedia
Clockwise, from top: American trucks crossing the 38th parallel, ... delivering “dummy”

nuclear bombs or heavy conventional bombs; the operation was ...
en.wikipedia.org/wiki/Korean_War - 312k - Cached - Similar pages

ACM TechNews Past Issues
Mar 6, 2006 ... The best-known attack method is differential power analysis (DPA), ... off the monitoring with dummy calculations or variable clock periods, ...
technews.acm.org/archives.cfm?fo=2006-03-mar/mar-06-2006.html - 46k - Cached - Similar pages

Life for dummies
The LeT itself has claimed responsibility of the attack on the Indian Parliament. ... George W Bush possesses the power to veto any congress and senate ...
vazutheterrible.blogspot.com/ - 78k - Cached - Similar pages

SNUG Boston 2006 Conference Registration Session Info
It also provides a methodology to do power analysis in this .... cells and designs requiring side channel attack resistance using a power balanced ...
https://www.snug-universal.org/SNUGReg/view.jsp?id=260 - 56k - Cached - Similar pages

[PDF] Security of Security Hardware
File Format: PDF/Adobe Acrobat - View as HTML
DES and RSA. Timing attack. Simple power analysis. Differential power analysis ... Example: the processing time is made constant by adding dummy cycles ...
soc.eurecom.fr/crypto/l1/l1.pdf - Similar pages

An Efficient High Performance Scalar Multiplication Method with ...
full power of timing attack'. Technical Report CG-2001/3, ... Solutions for Preventing Simple Side-Channel Analysis: Side- ...
index.ieeexplore.ieee.org/iel5/4488216/4493499/04493630.pdf - Similar pages

[PDF] Decorrelating Wireless Sensor Network Traffic To Inhibit Traffic ...
File Format: PDF/Adobe Acrobat - View as HTML
three hours when under a concerted traffic analysis attack, so we desire the ... Aggregator nodes are permitted and process data from their local sensor ...
www.cs.colorado.edu/~rhan/Papers/deng_traffic_pmc.pdf - Similar pages
by J Deng - Cited by 3 - Related articles - All 2 versions

[PDF] Design Challenges for a Differential-Power-Analysis Aware GALS ...
File Format: PDF/Adobe Acrobat - View as HTML
precise monitoring of the supply current. Furthermore the clock rates of the ... attack the power consumption of the. same operation needs to be measured ...
www.iis.ee.ethz.ch/async/pub/fmgals2005.pdf - Similar pages
by FK Gürkaynak - Related articles - All 2 versions

Sara's Guide to Writing a Good Lab Report
Use "dummy" data--placeholders for the data so that it will be clear if you .... When you write the analysis of a graph, follow this process: summarize the ...
www.cis.udel.edu/~sprenkle/acad/cisc372/labguide.html - 11k - Cached - Similar pages

[PDF] A-SSCC 2006 Advance Program www.a-sscc.org e Prog
File Format: PDF/Adobe Acrobat - View as HTML
the process. Moreover, such improvements as module reuse and calculation order ... it could resist 15000 less samples correlation power analysis attack. ...
www.el.gunma-u.ac.jp/analog/A-SSCC2006AdvanceProgram.pdf - Similar pages

[PDF] Towards a Formal Analysis of a Mix Network
File Format: PDF/Adobe Acrobat - View as HTML
the way to secure Mix implementations with dynamically controlled dummy traffic. ..... results of a FDR-based analysis, we chose to use FDR for the current ...
arkaptur.informatik.uni-freiburg.de/papers/2003/tr01.pdf - Similar pages

by B Wolff - Related articles - All 5 versions

SAS - Psychology of SAS | Encyclopedia.com: Dictionary Of Psychology
Statistical Analysis with Excel(TM) for Dummies ... The Oxford Pocket Dictionary of Current English as·sas·si·nate / ə□sasə□nāt / • v. ...
www.encyclopedia.com/doc/1O87-SAS.html - 79k - Cached - Similar pages

1 2 3 4 5 6 7 8 9 10 Next

"side channel" OR ((power OR current) analysis) attack dummy (operation (Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve | Try Google Experimental

Google Home - Advertising Programs - Business Solutions - Privacy - About Google